COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY SECURITY AUDIT GUIDELINE

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that they have the latest version of this ITRM publication. Questions should be directed to the VITA Policy, Practice and Architecture (PPA) Division. PPA will issue a Change Notice Alert, post on the VITA Web site and provide an e-mail announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers interested in the change.

This chart contains a history of this ITRM publication's revisions:

Version	Date	Purpose of Revision
Original	December 20, 2007	Base Document
Revision 1	03/15/2013	This update addresses the recent changes to IT security governance structure in the Commonwealth by aligning the Information Technology Security Audit Guideline with Information Technology Security Audit Standard. The guideline also includes new audit plan and corrective action plan templates.

Identifying Changes in This Document

- See the latest entry in the table above
- Vertical lines in the left margin indicate that the paragraph has changes or additions.
- Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

Review Process

Enterprise Solutions and Governance Directorate Review

Policy, Practices, and Architecture (PPA) Division provided the initial review of this publication.

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation
ITRM Guideline

Subject
Information Technology Security Audit Guideline

Effective Date
03/15/2013

Supersedes
COV ITRM Guideline SEC512-00 dated December 20, 2007

Scheduled *VITA* Review
One (1) year from effective date

Authority
Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

Scope
This Guideline is offered as guidance to all executive branch agencies, independent agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology databases or data communications in the Commonwealth. However, academic "instruction or research" systems are exempt from this Guideline. This exemption, does not, however, relieve these academic "instruction or research" systems from meeting the requirements of any other State or Federal Law or Act to which they are subject. This Guideline is offered only as guidance to local government entities.

Purpose
To guide agencies in the implementation of the information technology security audit requirements defined by ITRM Standard SEC502.

General Responsibilities
(Italics indicate quote from the Code of Virginia)

Secretary of Technology

Reviews and approves statewide technical and data policies, standards and guidelines for information technology and related systems recommended by the CIO.

Chief Information Officer of the Commonwealth (CIO)
Develops and recommends to the Secretary of Technology statewide technical and data policies, standards and guidelines for information technology and related systems.

Chief Information Security Officer (CISO)
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

Virginia Information Technologies Agency (VITA)
At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budgets requests and strategic plans, and when developing and managing IT related services.

Information Technology Advisory Council (ITAC)
Advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Executive Branch Agencies
Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems. Comply with the requirements established by COV policies and standards. Apply for exceptions to requirements when necessary.

In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Technology Strategies and Solutions Directorate the following duties: *"Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions."*

All Executive Branch, Legislative, Judicial Branches and Independent State Agencies and institutions of Higher Education
In accordance with §2.2-2009 of the *Code of Virginia,* To provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, procedures, and standards will apply to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs.

Related ITRM Policy and Standards
ITRM Policy, SEC500-02: Information Technology Security Policy (Revised 07/17/2008) (Superseded by SEC519-00)
ITRM Standard SEC501-06: Information Technology Security Standard (Revised 04/04/2011)
ITRM Standard SEC502-02: Information Technology Security Audit Standard (Revised 12/05/2011)

TABLE OF CONTENTS

1 Introduction

1.1 Information Technology Security

This Guideline presents a methodology for Information Technology (IT) security audits suitable for supporting the requirements of the *Commonwealth of Virginia (COV) Information Security Policy* (ITRM Policy *SEC519*), the *Information Security Standard* (ITRM Standard SEC501), and the *Information Technology Security Audit Standard* (ITRM Standard SEC502). These documents are hereinafter referred to as the "Policy", "Standard", and "Audit Standard", respectively.

The function of the Policy is to define the overall COV IT security program, while the Standard defines high-level COV IT security requirements, and the IT Security Audit Standard defines requirements for the performance and scope of IT security audits. This Guideline describes methodologies for agencies to use when meeting the IT security audit requirements of the IT Security Policy, Standard, and Audit Standard. Agencies are not required to use these methodologies, however, and may use methodologies from other sources or develop their own methodologies, if these methodologies meet the requirements of the Policy, Standard, and Audit Standard.

1.2 IT Security Audits

Information security audits are a vital tool for governance and control of agency IT assets. IT security audits assist agencies in evaluating the adequacy and effectiveness of controls and procedures designed to protect COV information and IT systems. This Guideline suggests actions to make the efforts of auditors and agencies more productive, efficient, and effective.

1.3 Roles and Responsibilities

Agencies should assign an individual to be responsible for managing the IT Security Audit program for the agency. While the individual assigned this *responsibility* will vary from agency to agency, it is recommended that this responsibility be assigned either to the agency Internal Audit Director, where one is available or to the Information Security Officer (ISO).

2 Planning

2.1 Coordination

As stated in the Audit Standard, at a minimum, IT systems that contain sensitive data*, or reside in a system with a sensitivity of high on any of the* criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years. *All IT security audits must follow either the generally accepted government auditing standards GAGAS Yellow Book (**Generally Accepted Government Auditing Standards**) or the international standards for the professional practice of internal auditing IIA Red Book (Institute of Internal Auditors' Standards).*

For maximum efficiency, the agency's IT Security Audit Program should be designed to place reliance on any existing audits being conducted, such as those by the agency's internal audit organization, Auditor of Public Accounts, or third party audits of any service provider. When contracting for sensitive systems to be hosted at or managed by a private sector third party service provider, a contractual term requiring compliance with the ITRM IT Security Policy and Standards should be included as well as a requirement that a third party conduct an IT Security audit on a frequency relative to risk should be included in the contract terms. Agencies should also consider including in contract terms qualifications for the IT Security Auditor such as those outlined in section 3.4 of this Guideline.

If multiple systems share similar characteristics such as use of the same logical access control method, database or infrastructure, the agency may wish to audit that common area once as a system rather than multiple times for each sensitive system that has a dependency. Similarly, if there is a sensitive system deployed at many locations a sampling of those locations may provide adequate assurance. Finally, if an agency has an active and defined control self assessment program in place that includes one or more sensitive systems, the agency may wish to place reliance on those self assessments, limiting the audit to evaluation and testing of key elements of the self-assessment(s).

2.2 IT Security Audit Plan

The IT security audit plan helps the agency schedule the necessary IT Security Audits of the sensitive systems identified in the data and system classification step in the risk management process.

The agency uses the IT security audit plan to identify and document the:

1. Sequencing of the IT Security Audits relative to both risk and the business cycle of the agency to avoid scheduling during peak periods;
2. Frequency of audits commensurate with risk and sensitivity; and
3. Resources to be used for the audit such as Internal Auditors, the Auditor of Public Accounts staff or a private firm that the agency deems to have adequate experience, expertise and independence. To provide adequate objectivity and separation of duties, IT security audits should not be performed by the same group or entity that created the IT security policies, procedures, and controls being audited, or that manage the IT operations.

An example of an IT Security Audit Plan is included in Appendix A.

3 Performance

As stated in the Audit Standard, prior to performing each IT Security Audit, the IT Security Auditor will contact the agency head or designee and agree on:

- A specific scope;
- A mutually agreeable schedule for the IT Security Audit;
- A checklist of information and access required for the IT Security Audit.

The level of access to information granted the auditor should be based on the principle of least privilege. The agency should designate an agency point-of-contact (POC) for the IT security audit; all auditor requests for access to agency information should be directed to the agency POC. An example checklist is included in Appendix C.

3.1 Scope

The scope of the audit defines boundaries of the project and should be established and agreed to by the agency prior to the conduct of the audit. As stated by the Institute of Internal Auditors: "the scope of the engagement should include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties." The scope defines what is planned to be assessed and/or tested in the audit for that system or systems and what period of time the audit will include as well as the timing of the audit itself. It also specifies any other control activity on which the auditor is placing reliance such as other audits or assessments.

The goal in defining the scope of the audit is to include within the audit all elements that are part of the IT system undergoing the audit and excluding those components that are external to the IT system being audited. In general, the scope of the audit should correspond to the system boundary of the IT system undergoing the audit. See the Standard, section 2.5, and the *ITRM Risk Management Guideline* (ITRM Guideline SEC506) for further information regarding IT system boundaries.

At a minimum, the audit scope must assess effectiveness of the controls and compliance with the Policy and Standard, as well as any other applicable Federal and COV laws and regulations such as:

- Internal Revenue Service (IRS) Regulation 1075; or
- The Privacy and Security rules of the Health Insurance Portability and Accountability Act (HIPAA).

Additionally, facets of controls other than compliance, including reliability and integrity of financial and operational information, effectiveness and efficiency of operations, and safeguarding of assets should be considered for inclusion within the scope of the audit depending on the IT system(s) being audited and relative risk.

3.1.1 Objectives

In addition to defining the Scope or boundaries of the IT Security Audit, the IT Security Auditor should also define the objectives of the audit. The objectives should define what will be determined within the scope of the audit. For example, an audit objective might be to determine whether access controls are functioning as intended and are adequately documented.

3.2 Schedule

To coordinate the impact across the organization, the agency should work with the auditor to establish an effective and workable schedule. The schedule should enable the audit to proceed in a logical progression and help coordinate the efforts of the auditor and involved

agency personnel. For example, if an audit will require disruption of an IT system, the schedule can be used to inform personnel and to minimize the impacts of the disruption.

3.3 Preparation for IT Security Audits

In preparation for conducting the IT Security Audit, the Auditor should familiarize themselves with any readily available material applicable to the audit such as laws, available reports, web related information, etc.

3.4 Qualifications of IT Security Auditors

As stated in the Audit Standard, IT Security Auditors are CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits. Agencies should consider the following qualifications for the selected IT Security Auditor:

- Familiarity with the COV IT Security Policy (ITRM Policy SEC519), IT Security Standard (ITRM Standard SEC501), and IT Security Audit Standard (ITRM Standard SEC502);
- Credentials as a Certified Public Accountant (CPA), Certified Internal Auditor (CIA), and/or Certified Information Systems Auditor (CISA); and
- Experience conducting IT audits within the past three to five years.

3.5 Documentation

The scope and objectives, schedule and information needed to complete the audit should be documented by the IT Security Auditor in an Engagement Letter or Memorandum to the agency head. An example IT Security Audit Engagement Letter is included in Appendix B.

3.6 Audit Process

Agencies are advised to define an audit process that includes the following phases:

- Familiarization – initial research and review of laws, policies, procedures and best practices
- Preliminary Survey – detailed information gathering phase which may include reviews of procedures, diagrams, the systems boundary definition, risk assessment and other existing documentation combined with interviews and/or surveys of key personnel, documentation of key controls, walkthroughs and observations, an initial assessment of key controls and design of the audit test plan;
- Fieldwork – Execution of the audit test plan and conclusions regarding the results. Any potentially negative conclusions should be confirmed with the agency's operations staff prior to escalation; and
- Reporting – Documentation of the audit results for management review and use.

Because the IT security audits within the Commonwealth span numerous subject areas extending to the wide variety of hardware platforms, software, integration methods, and business application areas in use, there is no one standard IT Security audit program that is

recommended. A general audit program is attached as an example in AppendixG. The general audit program identifies some sources for specific IT Security Audit technical considerations.

4 Documentation

4.1 Work Papers

Work papers comprise the notes and other intermediate work products that lead up to the auditor's final report. The auditor's work papers must document the audit and include sufficient evidence to support all conclusions. The auditor must protect the work papers in order to prevent compromise of the agency's security. The agency should support the auditor in the protection of audit work papers, which are comprised of notes the auditor has made during the audit, by providing appropriate protections, including locked files, access controlled facilities, etc.

4.2 Reports

The IT Security Audit Report documents the results of the audit. Audit results must be presented to the agency head or designee in a draft report for their review and comment. The agency head and auditor will collaborate to make mutually agreeable changes, and document the agency head's acceptance or non-acceptance of the findings.

4.3 Corrective Action Plan

As stated in the Audit Standard, a corrective action plan (CAP) must be prepared to document findings of the IT Security Audit. For each finding, the CAP documents whether or not the agency concurs with the finding and *shall include the*:

- *Planned corrective action; due date for the corrective action; and party responsible for the corrective action.*

For each finding with which the Agency does not concur, the plan shall include the:

- *Agency's statement of position; mitigating controls that are in place; and agency's acknowledgement of its acceptance of risk.*

Upon receipt of the plan, the IT Security Auditor shall incorporate the plan in the final IT Security Audit Report and present the final IT Security Audit Report to the Agency Head and the Agency Information Security Officer. An example Corrective Action Plan is included in Appendix D.

4.4 CAP Periodic Reporting

As stated in the Audit Standard, corrective action plans for all findings must be submitted to the CISO within 30 days of issuing the final audit report. An updated corrective action plan must be submitted quarterly (at the end of the quarter), until all corrective actions are completed. All corrective action plans and quarterly updates submitted must have evidence of agency head approval. Any modification to a corrective action for any IT Security Audit conducted by or on behalf of the Agency must be reported. In order to assist VITA in carrying out its information assurance responsibilities, agencies are requested to submit to the CISO each quarter the full audit report for each IT security audit conducted by or for the

agency during the previous quarter. If the report contains sensitive information, please do not email it but send an email to CommonwealthSecurity@VITA.Virginia.Gov requesting assistance on identifying an efficient yet secure manner of transmitting the report.

Glossary of Security Definitions

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at http://www.vita.virginia.gov/library/default.aspx?id=537

Appendices

These Appendices provide examples and templates for agencies to document their use of many of the methodologies described in this Guideline. *The Audit Plan and Corrective Action Plan templates are required for agencies to use by the Audit Standard SEC502 unless otherwise approved by the CISO* Each template consists of an example of the document, completed with fictional information. A blank version of the template for use by COV agencies can be found on the VITA website at http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs.

The examples use different fonts for instructions and example information, as follows:

- *Verdana* text is used for the template itself.
- **Shaded Arial Bold text** is example text.
- *Verdana Italic text* is provided as instructions for completing the template.

Appendix A – EXAMPLE /IT Security Audit Plan Template

Purpose: This Plan coordinate the execution of security audits for the IT systems supporting government databases (as defined by ITRM Standard SEC502-02).

Agency Information		**Contact Information**	
Agency Name	Budget Formulation Agency	**Name**	J [redacted]
Agency Acronym	BFA	**Title**	ISO
Agency Number	123	**E-mail**	[redacted]
Date of submission	01/02/2008	**Phone**	[redacted]

IT System Acronym *	**IT System Name**	**Planned Auditor**	**Date Last Audited (MM/YY)**	**Scheduled Audit Completion Date (Minimum once every 3 years)**			**Areas for Special Emphasis and Additional Audit Requirements**
				2008 (MM/YY)	**2009 (MM/YY)**	**2010 (MM/YY)**	
BFS	Budget Formulation System	The Auditing Firm	n/a	02/08		02/10	a) Security procedures for laptop use at employee homes. b) Policies regarding protection of mobile storage (flash drives, DVDs, etc.)
BCS	Budget Consolidation System	APA	05/06	5/08			a) IRS 1075 requirements. b) Requirements for users to complete background checks before receiving BCS access.
BRS	Budget Reconciliation system	BFA Internal Audit Staff	n/a	09/08	09/09	09/10	a) Security controls governing remote access to BRS data.

* If new system please indicate implementation date in the Areas for Special Emphasis and Additional Audit Requirements column.

NOTE: Agency Audit Plans should be submitted to Commonwealth Security by June 1 of each year.

Appendix A – Blank IT Security Audit Plan Template

Purpose: This Plan coordinate the execution of security audits for the IT systems supporting government databases (as defined by ITRM Standard SEC502-02).

Agency Information		**Contact Information**	
Agency Name		**Name**	
Agency Acronym		**Title**	
Agency Number		**E-mail**	
Date of submission		**Phone**	

IT System Acronym *	**IT System Name**	**Planned Auditor**	**Date Last Audited (MM/YY)**	**Scheduled Audit Completion Date (Minimum once every 3 years)**			**Areas for Special Emphasis and Additional Audit Requirements**
				2008 (MM/YY)	**2009 (MM/YY)**	**2010 (MM/YY)**	

* If new system please indicate implementation date in the Areas for Special Emphasis and Additional Audit Requirements column.

NOTE: Agency Audit Plans should be submitted to Commonwealth Security by June 1 of each year.

Appendix B – EXAMPLE / IT Security Audit Engagement Letter Template

March 30, 2008

[redacted]

The **Department of Citizen Services (DCS) Internal Audit Division (IAD)** is conducting the regularly scheduled IT security audit of the **DCS Request Processing System (RPS).**

The examination of **RPS** will be conducted in accordance with generally accepted internal auditing standards and will also meet the requirements of the Commonwealth of Virginia (COV) *Information Technology Resource Management (ITRM) Standard SEC502-02, Information Technology Security Audit Standard SEC501-06, and Information Technology Security Audit Standard SEC 502-02.*

Proposed Scope

The **RPS** System Audit will review the functioning of the **RPS** system for the period **October, 2007** through **April, 2008** and is scheduled to conclude by **June 30, 2008** with a total of **300** audit hours. The audit will be performed by [redacted] **Auditor**. The **RPS** system interconnects with system **MNO**. This audit excludes the **MNO** system but will include the **RPS** system up to the network interface point with the **MNO** system as well as the logical access controls between the systems. This audit includes the application layer as well as the infrastructure layer of the **RPS** system. The **RPS** System Audit does not include general end user Security Awareness Training or the incident response plan as these areas are covered in the regularly scheduled General Controls Audit.

Proposed Objectives

Overall, the **RPS** Audit will assess the effectiveness of controls over the **RPS** system and compliance with COV ITRM SEC500-02, IT Security Policy, COV ITRM SEC501-06, IT Security Standard, **DCS** IT Systems Management Procedures, any legal requirements and best practices. Specifically, the objectives of the **RPS** System Audit are to determine whether the IT security controls for the **RPS** system are documented and provide reasonable assurance that:

1. **Physical access to the production environment, stored data, and documentation is restricted to prevent unauthorized destruction, modification, disclosure, or use.**
2. **Logical access to the production environment, data files, and sensitive system transactions, is restricted to authorized users only.**
3. **The production environment is protected against environmental hazards and related damage.**

4. **Regularly scheduled processes that are required to maintain continuity of operations in the event of a catastrophic loss of data, facilities, or to minimize the impact of threats to data, facilities or equipment, are performed as scheduled.**

5. **Roles and responsibilities are adequately defined, documented and assigned to persons with an adequate technical training and role based IT Security technical training is planned and received.**

6. **System hardening measures have been applied to RPS adequate to protect RPS against risks to which it is exposed.**

7. **An Interoperability Security Agreement is in place for RPS covering data sharing with the MNO system.**

8. **Logging of IT security events is enabled for RPS, security logs are reviewed in a timely manner, and appropriate actions are taken by DCS IT staff in response to RPS security events.**

An Entrance Conference has been scheduled on **April 4, 2008** to discuss the proposed Scope and Objectives of the **RPS** System Audit further. At that time we will also need the contact points for the audit.

_____
Signature

[redacted]

_____
Name and Title

C: [redacted]

[redacted]

[redacted]

[redacted]

Date,

Agency Head Name
Agency Name
Street Address
City, State ZIP

The *IT Security Auditor* has agreed to conduct an IT security audit of the *IT System Name and Acronym.*

The examination of *IT System Acronym* will be conducted in accordance with *ITRM Standard SEC502-02, Information Technology Security Audit Standard*, and all other applicable IT security auditing policies and standards.

Proposed Scope

The *IT System Acronym* System Audit will review the functioning of the *IT System Acronym* system for the period *Period Start Date* through *Period End Date* and is scheduled to conclude by *Audit End Date* with a total of *Audit Effort* audit hours. The audit will be performed by *Audit Team Members*. The *IT System Acronym* system interconnects with system *Other IT System*. This audit excludes the *Other IT System Acronym* system but will include the *IT System Acronym* system up to the network interface point with the *Other IT System Acronym* system as well as the logical access controls between the systems. This audit includes the application layer as well as the infrastructure layer of the *IT System Acronym* system. The *IT System Acronym* System Audit does not include general end user Security Awareness Training or the incident response plan as these areas are covered in the regularly scheduled General Controls Audit.

Proposed Objectives

Overall, the *IT System Acronym* Audit will assess the effectiveness of controls over the *IT System Acronym* system and compliance with COV ITRM SEC500-02, IT Security Policy, COV ITRM SEC501-06, IT Security Standard and *Agency Acronym* IT Systems Management Procedures Specifically, the objectives of the *IT System Acronym* System Audit are to determine whether the IT security controls for the *IT System Acronym* system are documented and provide reasonable assurance that:

1. *IT Security Audit Objective #1.*
2. *IT Security Audit Objective #2.*
3. *IT Security Audit Objective #3.*
4. *IT Security Audit Objective #4.*

   Etc.

An Entrance Conference has been scheduled on *Entrance Conference Date* to discuss the proposed Scope and Objectives of the *IT System Acronym* System Audit further. At that time we will also need the contact points for the audit.

_____
Signature

Agency Internal Audit Director Name and Title

_____
Name and Title

C: *Agency IT Director Name and Title*

IT System Data Owner Name and Title

IT System Auditor Name and Title

Appendix C – EXAMPLE / IT Security Audit Checklist of Access Requirements Template

Agency	[redacted]		
System or Database	[redacted]		
Auditor	[redacted]		
Start Date	[redacted]	**Expected Completion Date**	[redacted]

Access to the following resources will be made available to the auditor upon request:

Resource	Contact	Phone
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

A copy of all related agency policies and procedures will be needed as well as job descriptions or contracts for all persons involved with the system other than end users.

Agency Approval

SIGNATURE

NAME AND TITLE

[redacted]

Agency			
System or Database			
Auditor			
Start Date		**Expected Completion Date**	

Access to the following resources will be made available to the auditor upon request:

Resource	Contact	Phone

Agency Approval

SIGNATURE

NAME AND TITLE

Appendix D – EXAMPLE / Corrective Action Plan and IT Security Audit Quarterly Summary Template

> ***PURPOSE:*** *This Plan describes IT Security Audit findings; documents responsibility for addressing the findings; and describes progress towards addressing the findings. Provide enough information to enable the reader to understand the nature of the finding, the impacts, and the planned remedy*.

Submission Date:	**04/15/08**

Audit Name:	**Budget Formulation System (BFS) BFA-001: Issued 03/08**							
IT System Names(s)	**Budget Formulation System**							
Audit Finding No.	**SEC501-07 Control Number**	**Summary**	**Agency Concurs [1]**	**Planned Corrective Action or Mitigating Controls [2]**	**Responsible Person(s)**	**Status [3]**	**Due Date**	**Exception on File [4]**
1	**MP-1-COV #2**	**BFA should develop & enforce policies & procedures requiring agency Head approval for storage of sensitive BFS data on mobile devices, including employee laptops, USB drives, DCs, & DVDs.**	**Concurs**	**Policies & procedures have been developed; implementation is underway &will be completed this month.**	**John James**	**U**	**09/08**	**N**
2	**AC-2-COV #2**	**BFA should enforce existing agency procedures to remove unneeded accounts from BFS**	**Concurs**	**Procedures for removal of unneeded BFS accounts are now being enforced; review of all BFS accounts to identify & remove unneeded accounts is underway & will be completed this month.**	**Bill Michaels** **Michael Williams**	U	**09/08**	N
3	**IA-5 CESS #1 (d)**	**BFA should enforce existing agency requirements for password changes every 90 days on BFS**	**Concurs**	**BFS has been reconfigured to require password changes every 90 days.**	**John James**	C	**09/08**	N

Audit Name:	Budget Consolidation System (BCS) BFA-002: Issued 04/08							
IT System Names(s)	Budget Consolidation System							
Audit Finding No.	**SEC501-07 Control Number**	**Summary**	**Agency Concurs**	**Planned Corrective Action or Mitigating Controls**	**Responsible Person(s)**	**Status**	**Due Date**	**Exception on File**
1	**AC-2-COV #10 (b)**	**BFA should enforce policies & procedures requiring BCS users to complete criminal background checks before receiving access to the BCS, due to the sensitivity of BCS data.**	**Does Not Concur**	**BFA believes that screening during hiring process sufficiently mitigates the risk of giving users access to BCS while background checks are underway as such checks are concluded within one week.**	**John Davis**	**NS**	**N**	

[1] Agency Concurs: Concur or Does Not Concur
[2] If the Agency does not concur, the Mitigating Controls and Risk Acceptance must be stated in Planned Corrective Action.
[3] Status: NS = Not Started; U = Underway; C = Completed
[4] Exception on file for findings not compliant with COV Information Security Standard (SEC501): Y = Yes; N = No

NOTE: CAPs must be submitted within 30 days of issuing the final audit report completion. All CAPs should be combined into one cumulative summary agency CAP and submitted to Commonwealth Security quarterly within 30 days of quarter's end date to be counted.
This sheet is protected with no password.

Appendix E - Corrective Action Plan and IT Security Audit Quarterly Summary Template excel.xlsx

Corrective Action Plan and *IT Security Audit Quarterly Summary* Template

PURPOSE: This Plan describes IT Security Audit findings; documents responsibility for addressing the findings; and describes progress towards addressing the findings. Provide enough information to enable the reader to understand the nature of the finding, the impacts, and the planned remedy.

Submission Date:	

Audit Name:								
IT System Names(s)								
Audit Finding Number	SEC501-07 Control Number	Summary	Agency Concurs [1]	Planned Corrective Action or Mitigating Controls [2]	Responsible Person(s)	Status [3]	Due Date	Exception on File [4]

Audit Name:								
IT System Names(s)								
Audit Finding Number	SEC501-07 Control Number	Summary	Agency Concurs	Planned Corrective Action or Mitigating Controls	Responsible Person(s)	Status	Due Date	Exception on File

[1] Agency Concurs: Concur or Does Not Concur
[2] If the Agency does not concur, the Mitigating Controls and Risk Acceptance must be stated in Planned Corrective Action.
[3] Status: NS = Not Started; U = Underway; C = Completed
[4] Exception on file for findings not compliant with COV Information Security Standard (SEC501): Y = Yes; N = No

NOTE: CAPs must be submitted within 30 days of issuing the final audit report completion. All CAPs should be combined into one cumulative summary agency CAP and submitted to Commonwealth Security quarterly within 30 days of quarter's end date to be counted.
This sheet is protected with no password.

Appendix F - Corrective Action Plan and IT Security Audit Quarterly Summary Template Word.docx

Corrective Action Plan and *IT Security Audit Quarterly Summary* Template

PURPOSE: This Plan describes IT Security Audit findings; documents responsibility for addressing the findings; and describes progress towards addressing the findings. Provide enough information to enable the reader to understand the nature of the finding, the impacts, and the planned remedy.

Submission Date:	Select Date

Audit Name:	Click here to enter text.							
IT System Name (s):	Click here to enter text.							
Audit Finding Number	**SEC501-07 Control Number**	**Summary**	**Agency[1] Concurs**	**Planned Corrective Action or Mitigating Controls[2]**	**Responsible Person(s)**	**Status[3]**	**Due Date**	**Exception on File[4]**
Enter #	Enter Number	Summary	Choose an item.	Click here to enter text.	Enter Name	Choose an item.	Select Date	Choose an item.
Enter #	Enter Number	Summary	Choose an item.	Click here to enter text.	Enter Name	Choose an item.	Select Date	Choose an item.
Enter #	Enter Number	Summary	Choose an item.	Click here to enter text.	Enter Name	Choose an item.	Select Date	Choose an item.

Audit Name:	Click here to enter text.							
IT System Name (s):	Click here to enter text.							
Audit Finding Number	**SEC501-07 Control Number**	**Summary**	**Agency Concurs**	**Planned Corrective Action or Mitigating Controls**	**Responsible Person(s)**	**Status**	**Due Date**	**Exception on File**
Enter #	Enter Number	Summary	Choose an item.	Click here to enter text.	Enter Name	Choose an item.	Select Date	Choose an item.
Enter #	Enter Number	Summary	Choose an item.	Click here to enter text.	Enter Name	Choose an item.	Select Date	Choose an item.
Enter #	Enter Number	Summary	Choose an item.	Click here to enter text.	Enter Name	Choose an item.	Select Date	Choose an item.

[1] Agency Concurs: Concur or Does Not Concur
[2] If the Agency does not concur, the Mitigating Controls and Risk Acceptance must be stated in Planned Corrective Action.
[3] Status: NS = Not Started; U = Underway; C = Completed
[4] Exception on file for findings not compliant with COV Information Security Standard (SEC501): Y = Yes; N = No

NOTE: CAPs must be submitted within 30 days of issuing the final audit report completion. All CAPs should be combined into one cumulative summary agency CAP and submitted to Commonwealth Security quarterly within 30 days of quarter's end date to be counted.

This form is protected with no password. 1

Appendix G – General Audit Program Example

II. PRELIMINARY SURVEY

Objective: To adequately plan the audit & obtain background information for the activities to be audited including researching past reports, applicable laws, policies and standards as well as best practices.

	Audit Step	W/P No	Est. Hrs	Act. Hrs
A.	1. Document planning meeting the Internal Audit Director or agency representative. Obtain name of system, identification of previous reviews, and applicable laws, policies and standards, and related documentation such as the system boundary definition, any interconnectivity with other systems, system risk assessment and system roles and responsibilities. 2. List draft major Scope (including System(s) Names), Objective or Resources decisions including any technical assistance needed and any coordination with the Auditor of Public Accounts (APA). _____ _____ _____ _____ _____ 3. Is APA Coordination Needed? **YES** **NO** IF "YES" State what, when & who: _____ _____ _____ for Year Ending _____, 20xx Meeting date – _____, 20xx, Representing 4. Is technical Assistance Needed? (circle) **YES** **NO** IF "YES" State what, when, who & estimated cost: _____ _____			
B.	Prepare Date & Time Budget (time in columns to right) : **Phase** **Deadline** **Budget** Familiarization x/xx/20xx xx.x Preliminary Survey x/xx/20xx xx.x Fieldwork x/xx/20xx xx.x			

	Audit Step			W/P No	Est. Hrs	Act. Hrs
	Draft Report	x/xx/20xx	xx.x			
	Final Report	x/xx/20xx	xx.x			
	Administration	x/xx/20xx	xx.x			
	TOTALS:		**xxx.x**			
	Time reports should be included in the work papers behind the Date and Time Budget.					
C.	Prepare Engagement Memorandum signature & include: proposed review scope & objectives, 1. estimated starting & completion dates, 2. Auditor-in-Charge (AIC) & staffing, 3. physical facilities required, if any, & 4. general questionnaire of background information needed & timeframe for receipt.					
D.	Review and document any applicable IA reports, APA reports & any reports issued from other sources such as Agency, DPS Review Team, JLARC, Consultants, etc. List any issues and dispositions related to the system or the general control environment that might be pertinent.					
E.	Review and document any Federal or State laws pertinent to the system as well as the Commonwealth IT Security Policies and Standards http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs					
F.	Review and document pertinent industry information technology guidance from the Institute of Internal Auditors, ISACA and the AICPA as well as from organizations such as: 1. CobiT from the IT Governance Institute: http://www.itgi.org/ 2. National Institute of Standards & Technology Computer Security Division: http://csrc.nist.gov/ 3. International Standards Organization Guidance on Information Security http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm 4. AuditNet - Kaplan's comprehensive KARL (audit resource list) and ASAP (auditors sharing audit programs) site http://www.auditnet.org/					
G.	Review and document Agency internal policies & procedures, Division/Staff unit policies & procedures, etc. & complete.					
H.	Schedule & conduct an entrance conference with applicable Agency Management to discuss proposed scope & objectives, recent or proposed changes in the audit area, legislative & financial concerns, key contacts, audit timing & staffing. Document in a memo.					
I.	Submit Familiarization work papers for review and clear review notes.					
	Total For Familiarization					

II. PRELIMINARY SURVEY

Objective: To obtain an understanding of the IT System area being audited including goals & objectives, regulations, & areas of management concern.

	Audit Step	W/P No	Est. Hrs	Act. Hrs
A.	Gain knowledge of the area being audited by reviewing related documents, conducting interviews & observing the processes & functions. Obtain the organizational chart of the area being audited and the job descriptions of staff members. List the major segments/processes of your review below and reference to the detailed narratives or flowcharts for each. Include completed samples of input & output documents, forms & report. Include source on samples. Obtain auditee sign off on narratives and flowcharts to ensure accurate representation. 1. Major Process 1 2. Major Process 2 3. Major Process 3 4. Major Process 4 5. Major Process 5 6. Major Process 6			

	Audit Step	W/P No	Est. Hrs	Act. Hrs
B.	Analyze the strengths and weaknesses of the major processes in the narratives and flowcharts. Prepare a Risk Matrix that identifies the following for each preliminary audit objective: - the risks and expected controls for each objective - actual practices that fulfill each element (strength) or the absence of such (weakness) with work paper reference to the flowchart or narrative and - the disposition for each actual practice listed as appropriate from one of the following: report without testing, Detailed Fieldwork Program reference or no further action (NFA) as outside scope or immaterial.			
C.	Prepare a summary of proposed modifications to the audit scope & objectives & prioritize the objectives in order of significance.			
D.	Develop the Detailed Fieldwork Program to include test steps for each objective as well as the sampling plans. Estimate time for audit steps & calculate completion date – document detailed time on by step and total time and the deadline on **I. B.** Reference the applicable audit steps on the risk matrix. If necessary, draft proposed revisions to budget & report due date & submit or approval – include on this General Audit Program.			
E.	If there are revisions to the audit scope, objectives, report due date or other areas of significance based on preliminary survey, prepare a memorandum to the attendees of the Entrance Conference to communicate the changes.			
F.	Prepare a Conclusion Summary for inclusion in the report for items which will not be addressed in fieldwork & discuss with operating manager(s) & obtain signature(s).			
G.	Submit work papers, detailed fieldwork program & Permanent File for review and clear any resulting review notes.			
	Total Hours For Preliminary Survey			
	FAMILIARIZATION & PRELIM. SURVEY: Date Completed _____Total Hrs:			

III. FIELDWORK

Objective: To collect, analyze, interpret, & document sufficient, competent, & relevant information as outlined in the detailed fieldwork program to support audit results & ensure that the audit objectives are achieved.

	Audit Step	W/P No.	Est. Hrs.	Act. Hrs.
A.	Perform testing as specified on the Detailed Fieldwork Program (total estimated time should be listed here). When completed, record actual total testing time here. Ensure that testing results are discussed with affected personnel as encountered. Do not document results in Conclusion Summaries without first discussing the issues with applicable operating managers to ensure their awareness & the auditor's complete understanding.			
B.	For each testing section prepare a Conclusion Summary stating objective, conclusion, procedures & summary of the prioritized results of testing which substantiate conclusions. Cross reference results to detailed W/P's. Include proposed disposition; place "Verbal" points last.			
C.	Review work to ensure that work papers are complete: 1. Has a heading, states name of the function examined, description of the contents of the work paper, period of the audit, & detailed fieldwork program step performed. 2. page number, initial & date (1st page of series) 3. States purpose, source, scope & conclusion, 4. Are adequate to support conclusions, and 5. Conclusion Summary Sheets are cross-referenced to support.			
D.	Submit working papers & the permanent file for review & clear subsequent review notes.			
E.	Discuss Conclusion Summary Sheets with operational managers and directors, document the results, revise Sheets & index as necessary.			
	FIELDWORK: Date Completed _____Total Hours:			

IV. REPORTING

Objective: To communicate the results of the audit to management.

	Audit Step	W/P No.	Est. Hrs.	Act. Hrs.
A.	Prepare a Draft Report: 1. Write report introduction, background & scope. 2. Consolidate conclusion summaries into a report, x-ref 3. Write memo for less significant items. 4. Submit report for review & clear review notes. 5. Set up the Exit Conference and distribute Draft Report 6. Conduct Exit Conference to brief on the audit results and request a date for completion of the corrective action plan. (Note: If any material changes to the audit report are identified, establish the date for revised report to be issued.)			
B.	Obtain Corrective Action Plan 1. Analyze the Corrective Action Plan for adequacy and document. 2. Advise agency management of any apparent inadequacies in the Corrective Action Plan & resolve.			
C.	Prepare a Final Report: 1. Add the revised Corrective Action Plan to the revised Draft Report to prepare the Final Report. 2. Submit report for review & clear review notes. 3. Distribute the final report.			
	REPORTING: Date Completed _____Total Hours:			